A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Nozomi Networks, Inc.

Year:
2025

NOZOMI NETWORKS

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

February 16, 2024 to March 15, 2025

Table of Contents

SECTION 1

ASSERTION OF NOZOMI NETWORKS, INC. MANAGEMENT

ASSERTION OF NOZOMI NETWORKS, INC. MANAGEMENT

May 15, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Nozomi Networks, Inc.'s ('Nozomi Networks' or 'the Company') OT and IoT Security and Visibility Services System throughout the period February 16, 2024 to March 15, 2025, to provide reasonable assurance that Nozomi Networks' service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Availability, and Confidentiality (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Nozomi Networks, Inc.'s Description of Its OT and IoT Security and Visibility Services System throughout the period February 16, 2024 to March 15, 2025" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 16, 2024 to March 15, 2025, to provide reasonable assurance that Nozomi Networks' service commitments and system requirements were achieved based on the Trust Services Criteria. Nozomi Networks' objectives for the system in applying the applicable Trust Services Criteria are embodied in its service commitments and system requirements relevant to the applicable Trust Services Criteria. The principal service commitments and system requirements related to the applicable Trust Services Criteria are presented in "Nozomi Networks, Inc.'s Description of Its OT and IoT Security and Visibility Services System throughout the period February 16, 2024 to March 15, 2025".

Nozomi Networks uses Amazon Web Services, Inc. ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nozomi Networks, to achieve Nozomi Networks' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Nozomi Networks' controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Nozomi Networks' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Nozomi Networks' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents the applicable Trust Services Criteria and the complementary user entity controls assumed in the design of Nozomi Networks' controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period February 16, 2024 to March 15, 2025 to provide reasonable assurance that Nozomi Networks' service commitments and system requirements were achieved based on the applicable Trust Services Criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Nozomi Networks' controls operated effectively throughout that period.

Karen Meohas

Karen Meohas
Director of Governance, Risk, and Compliance
Nozomi Networks, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Nozomi Networks, Inc.:

Scope

We have examined Nozomi Networks' accompanying assertion titled "Assertion of Nozomi Networks, Inc. Management" (assertion) that the controls within Nozomi Networks' OT and IoT Security and Visibility Services System were effective throughout the period February 16, 2024 to March 15, 2025, to provide reasonable assurance that Nozomi Networks' service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Availability, and Confidentiality (applicable Trust Services Criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Nozomi Networks uses AWS to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nozomi Networks, to achieve Nozomi Networks' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Nozomi Networks' controls, the applicable Trust Services Criteria, and the types of complementary subservice organization controls assumed in the design of Nozomi Networks' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nozomi Networks, to achieve Nozomi Networks' service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Nozomi Networks' controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of Nozomi Networks' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Nozomi Networks is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Nozomi Networks' service commitments and system requirements were achieved. Nozomi Networks has also provided the accompanying assertion (Nozomi Networks assertion) about the effectiveness of controls within the system. When preparing its assertion, Nozomi Networks is responsible for selecting, and identifying in its assertion, the applicable Trust Services Criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable Trust Services Criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

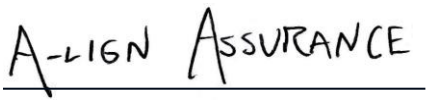
In our opinion, management's assertion that the controls within Nozomi Networks' Services System were suitably designed and operating effectively throughout the period February 16, 2024 to March 15, 2025, to provide reasonable assurance that Nozomi Networks' service commitments and system requirements were achieved based on the applicable Trust Services Criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Nozomi Networks' controls operated effectively throughout that period.

The SOC logo for Service Organizations on Nozomi Networks' website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Nozomi Networks, user entities of Nozomi Networks' Services System during some or all of the period February 16, 2024 to March 15, 2025, business partners of Nozomi Networks subject to risks arising from interactions with the OT and IoT Security and Visibility Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tampa, Florida
May 15, 2025

SECTION 3

NOZOMI NETWORKS, INC.'S DESCRIPTION OF ITS OT AND IOT SECURITY AND VISIBILITY SERVICES SYSTEM THROUGHOUT THE PERIOD FEBRUARY 16, 2024 TO MARCH 15, 2025

OVERVIEW OF OPERATIONS

Company Background

Nozomi Networks was founded in 2013 with the goal to develop cyber-security visibility solutions for industrial control systems (ICS) using Operational Technology (OT). The Nozomi Networks Solution includes different types of network sensors including Guardians, Guardian Air, Central Management Console (CMC), and ARC endpoints, and Vantage SaaS. The Guardian and CMC products were originally developed using on-premises appliances and have since expanded to include global management functionality as a software as a service (SaaS) solution, Vantage.

The products are developed and deployed as embedded software in on premises appliances, remote collectors, or personal computers at large scale industrial and manufacturing installations.

The original Guardian product has since evolved to include support for Internet of Things (IoT) technologies, ARC for data collection, and Vantage, the global SaaS management system.

The organization is headquartered in San Francisco, California (United States), with engineering and technical operations in Mendrisio (Switzerland).

Nozomi Networks has achieved a leadership position for industrial cyber-security visibility solutions in several vertical industries that include energy, pharmaceutical, mining, utilities, automotive, airport operations, and manufacturing.

Description of Services Provided

Nozomi Networks provides Vantage as a global cloud-based SaaS solution which works in conjunction with an installed base of one or multiple Sensors (Guardian / CMC) appliances, Guardian virtual instances, Guardian Air, Remote Collectors, and ARC endpoint sensors.

The service unifies the management of multiple sensor deployments into a single web interface and provides global visibility, vulnerability reports, and detection of cyber threats in the customer OT and IoT networks.

The Vantage service is presented as a web portal and designed for self-management by the customer, which includes easy application programming interface (API) integration of Sensor deployments with Vantage, the integration of Security Assertion Markup Language (SAML)-based Single Sign-On (SSO) and certificate authorities for enterprise customers.

Vantage aims to provide real-time asset activity information, alerting, and vulnerability reporting of the customers' global asset deployments. This requires a centralized sensor data repository, which is subject to strict confidentiality requirements and protection controls.

The service is available in multiple geographic regions with customer selectable data storage locations.

Customers manage deployed sites with registered network sensors, view the asset inventory, receive, analyze, and respond to alerts and vulnerability reports. Monitoring is performed in real-time to support continual monitoring, or from selectable sets of previous events.

Advanced behavioral anomaly detection features and in-depth detailed risks and threat information of the deployed on premises Sensor product are presented in Vantage at a summary level.

Vantage offers different methods organizing the asset views, by tagging and grouping options, alerting rules, and audit log capabilities for relevant systems activities which are customizable to the requirements of the customer environment.

Vantage allows the operations of multiple role-based user groups and privileges, including a master administrator account created by Nozomi Networks during the onboarding process.

Customers can acquire optional services such as Threat Intelligence, which delivers a single, unified source of threat data on the latest emerging threats and vulnerabilities. Threat data includes malicious Internal Protocol (IP) addresses or URLs, new indicators of compromise signatures, threat sources, malware hashes, and methods and tactics to gain system access.

Additional Asset Intelligence enhances device profiles, enabling teams to make informed decisions about maintenance and security of their OT and IoT devices. Asset Intel helps enrich existing high confidence data collected by other data sources with information that cannot be found in communication.

Principal Service Commitments and System Requirements

Vantage is designed to support customer security operations with an infinitely scalable number of sensor instances and assets under control.

To achieve economy of scale, the Vantage service leverages the power of cloud computing as a multi-tenant and highly available service.

Vantage aims to provide real-time asset activity information, alerting, and vulnerability reporting of the customers' global asset deployments. This requires a centralized sensor data repository, which is subject to strict confidentiality requirements and protection controls.

Vantage uses the multi-tenant cloud model while ensuring data segregation across multiple customers, encryption of data in transit and at rest, and reliance on robust security frameworks of the Infrastructure as a Service (IaaS) providers.

The infrastructure of Vantage has been designed to be protected by several layers of protection. Anti-distributed denial-of-service (DDOS), web application firewalls (WAFs), load balancers, firewalls, gateways, service meshes and intrusion detection systems (IDS) act at the network level to sit between the external public Internet and the inner components of the system. Compute nodes run on hardened configurations, data stores are encrypted, communications are encrypted, and controls are put in place to log activity in the system and notify our security and information event management (SIEM) system.

The architecture is secure by design. Customers access the system from the outermost component, the Content Delivery Network (CDN) - which also acts as WAFs and Anti-DDOS. Through other internal networks/virtual private clouds (VPCs) the traffic reaches the hearth of the system - the Kubernetes cluster, where requests are processed. The compute side of the cluster is shared among customers: it has been designed to be stateless and not hold any data.

The data tier is separated per customer: each Customer has its own scalable data tier to guarantee a logical and "physical" separation of data. There is also a shared data tier that is used by the system to orchestrate requests. The Customer-private data tier can only be accessed by the compute nodes, and from specific containers (pods) of the Kubernetes cluster. From the outside, the data tier is protected by SAML 2.0 Single Sign On (which is secured on the Customer side with multifactor authentication (MFA)) so that only users with a valid Customer domain's account can access the system and thus the data contained in the private data tier.

In the entire system, each customer has its own Customer ID. Each customer can create one or more isolated data containers called Organizations, each with a dedicated and globally unique Organization ID. Users live inside the Customer-private data tier and have a local user ID there.

When a user logs into the system, it is recognized by a session token that is bonded to its customer and organization ID. Based on this information, the compute nodes can process the request in isolation and connect to the right data tier.

Encryption in Vantage is implemented at various layers and occurs multiple times. Access to the Vantage web interface is restricted to Hypertext Transfer Protocol Secure (HTTPS) connections only, utilizing TLS 1.2 or TLS 1.3, with strong encryption algorithms.

Internal network traffic between the different environment components is secured using TLS 1.3. Each customer has a dedicated database. A unique key, stored in a Key Management System (KMS), is used for this encryption and is rotated once a year.

The application functions within a completely encrypted environment, implementing encryption for data stored on disk, during network transfers, and in host memory. Furthermore, Nozomi Networks uses an envelope encryption strategy for sensitive data at the application level, creating a unique random session key for each encryption request.

Vantage is available in multiple regulatory data regions, with each region operating independently and without sharing data with one another.

Only a small subset of engineering team members is authorized to manage customer data. Activities involving customer data are approved, monitored, and subject to compliance audits.

Security and privacy commitments to customers are documented and communicated in contractual agreements, the Service Level Agreements (SLA), and Data Protection Authority (DPA) addendums.

The security practices for the design and operations of the Vantage services include, but are not limited to:

- Access to information is restricted based on defined roles in the system.
- Access to customer data is controlled and authorized by the customer.
- Use of encryption of data in transit and at rest.
- Conformance with best security practices, including peer review.
- Robust supply chain risk management system.
- Software development methods are based on agile, scrum and extreme programming techniques.
- Continuous vulnerability assessments embedded in the release process.
- Periodic third-party penetration testing.
- Release of bug-free software into production.

Nozomi Networks establishes operational security requirements for both product development and internal operations of the Vantage SaaS from multiple sources, which include global cyber-intelligence communities, government agencies, and an internal research department focused on cyber-risk analysis and intelligence.

Internal security requirements are documented and adopted by Nozomi Networks' management in the information security management system (ISMS) framework, which include requirements for relevant controls designed to govern how the development, engineering, operations, protection of customer data and support of the Vantage service is managed. It also includes the necessary selection and training of the personnel.

Components of the System

Infrastructure

The infrastructure supporting the organization's OT and IoT Security and Visibility Services System is architected with a strong emphasis on security, reliability, and scalability. It is built on a foundation of cloud-native technologies and distributed systems that ensure high availability and performance across global regions.

Identity and access management is centrally governed to enforce strict authentication and authorization controls for users and devices. Web-facing applications are protected by multiple layers of defense to detect and mitigate malicious activity, while content delivery is optimized through a globally distributed network to ensure low-latency access and resilience.

Real-time monitoring and alerting mechanisms are in place to track system health and performance, enabling rapid response to anomalies. Cryptographic key management is handled through secure, centralized services that support encryption of data at rest and in transit, ensuring confidentiality and integrity.

The infrastructure leverages container orchestration to manage microservices efficiently, supporting rapid deployment and scalability. Load balancing mechanisms distribute traffic intelligently to maintain service continuity and responsiveness.

Data storage solutions are designed for durability and performance, supporting both structured and in-memory data needs. These systems are optimized for secure storage of customer data and application metadata, as well as for high-speed caching and message brokering to support real-time operations.

Software

The infrastructure and software supporting the organization's OT and IoT Security and Visibility Services System are designed with a strong emphasis on security, reliability, and operational efficiency. The infrastructure leverages cloud-native technologies to ensure high availability, secure access control, and real-time monitoring. It incorporates encrypted data handling, automated load balancing, and scalable microservice orchestration to maintain service continuity and protect sensitive information. Data storage and caching systems are optimized for performance and resilience, supporting both structured and real-time data needs.

On the software side, the environment is built using modern, secure frameworks and tools that enable seamless system connectivity, efficient backend processing, and responsive user interfaces. Workflow automation and deployment pipelines are integrated to ensure consistent, secure, and traceable software delivery. Documentation and onboarding processes are streamlined through dedicated platforms, enhancing operational transparency and reducing risk. Together, these components form a cohesive, secure, and scalable foundation that aligns with industry best practices and supports the delivery of high-assurance services.

People

Nozomi Networks has a staff of approximately 300 employees worldwide, with 30% of personnel directly or indirectly supporting Vantage. The staffing is organized in the following functional areas:

Corporate: Executives, business operations staff such as legal, compliance, human resources (HR), training, and corporate information technology (IT). Through personnel, product quality and security control performance reporting, Nozomi Networks tracks internal metrics to assess overall achievements and business objectives, which are reported to various external stakeholders.

Product Managers (PMs): PMs organize product features, enhancements, bug remediation activities and product releases using a standardized methodologies and processes. PMs collaborate with customers, field engineers, engineering management and technical support on features and release timelines.

Sales Engineers (SEs): Proof of concepts are arranged and conducted for the products and services with prospective customers.

Site Reliability Engineers (SREs): Manage the availability, performance, and security of the Vantage product. This includes patch and vulnerability management, incident response, root cause analysis, quality assurance monitoring, disaster recovery, and automation solutions across the application deployment for the optimization of cloud services.

Technical Support Engineers (TSEs): Receive customer requests via support portal, email, phone call in the form of support cases. TSEs troubleshoot issues with customers to determine the best course of action. If an issue is determined to be a defect or a bug, Support reports to Engineering for a workaround or a fix. If the issue relates to infrastructure, TSE contacts SRE immediately for resolution. Corrections and changes are documented in a tracking system.

Platform Engineers (PEs): Manage the cloud services infrastructure access to Vantage for authorized Nozomi Networks Employees, and support systems for the product development teams. This includes disaster recovery and other business continuity programs for physical assets.

Software Development Engineers (SDEs): Develop and maintain the product software for Nozomi Networks. This includes Vantage, third-party services, and the external websites that interact with the Vantage. The staff includes software developers, SEs, software quality assurance and deployment engineers.

Product Security Engineers (PSEs): Conduct periodic third-party penetration testing, maintain continual vulnerability scanning, manage the software bill of materials (SBOM), the security and legal use of third-party components and maintains membership with the MITRE organization for participation in the global threat intelligence community.

Corporate IT: Helpdesk, systems administration, applications support, information security, and operations to manage application interfaces of business applications, providing day to day support to internal end users that either develop or support Vantage products. Supports the personnel with consolidated monitoring for internal and external security threats, manages end-point protection and maintains the inventory of information assets.

Governance, Risk, and Compliance: The GRC function at Nozomi Networks plays a pivotal role in safeguarding the organization’s integrity, trust, and regulatory alignment by orchestrating a comprehensive framework that spans information security, data privacy, corporate governance, and audit readiness. The team ensures compliance with global standards through rigorous documentation, policy oversight, and third-party risk management, while also supporting product and brand credibility via certifications and customer assurance programs.

Human Resources: The Human Resources team supports information security by conducting pre-employment background checks, managing onboarding processes that include NDA signing and mandatory security training, and ensuring timely offboarding with access revocation. They also oversee ongoing security awareness through annual training and policy acknowledgments to maintain a culture of accountability and compliance.

Data

The Vantage service is deployed as a SaaS platform that allows Customers to monitor and analyze their globally deployed Guardian sensors using a centralized interface.

The customer managed Guardian sensors are configured to transmit data upstream to Vantage. Vantage provides a secure environment for the transmission, processing, and storage of customer data. The selection of data transmitted to Vantage is determined by the Customer.

Vantage organizes the view of the data by:

- Sites
- Sensors

- Assets
- Alerts
- Vulnerabilities
- Threat Content
- Process Variables
- Traffic
- Reports

Processes, Policies and Procedures

Nozomi Networks has established a formal ISMS policy and procedure framework that describes the security requirements of the company operations relevant to the Vantage product operations, including logical access, systems operations, change control, encryption requirements and secure software development procedures. Business groups are required to adhere to the policy framework and procedures. Specific procedures define how services are managed for customer delivery. Policies and procedures are located on the Company's Intranet and can be accessed by any Nozomi Networks team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system.

Please see the "Subservice Organization" section below for a detailed listing of controls owned by AWS.

Logical Access

Vantage requires customer credentials to be added to the platform during the onboarding process. When added, Vantage uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected using the native system security functions that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

Vantage allows integration of the authentication and authorization process with federated identity management systems, which are under control of the customer.

Customers access Vantage services through the Internet using transport layer security (TLS) encrypted connections. Within the customer organization, system users supply valid user credentials to gain access to the Vantage application instance. Passwords conform to password configuration standards and MFA can be enabled. Customers can delegate the sign-in functionality to an external SSO service, which allows authentication and authorization to be accepted by Vantage from authorized external sources.

For back-end access, including access to customer data for support purposes, authorized Nozomi Networks employees sign on using Active Directory managed user ID's, passwords and a token-based MFA system.

Customer data access is authorized only after explicit consent is granted by the customer. Passwords conform to defined password standards and are enforced through parameter settings in AD. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts.

Upon hire, employees have assigned responsibilities according to the position and job function in the HR management system. If the employees need access to the platform the manager approves a ticket and assigns a task to the PE which will grant the appropriate privilege. Access rules have been pre-established based on the defined access roles.

Terminated employees have their accounts disabled when HR has issued a termination ticket to IT. Once disabled, employees can no longer access the system. Logical access reviews to validate the completion of access credential removals are performed on at least an annual basis.

Computer Operations - Backups

A continuous backup strategy is applied to the system to persist the data in a disaster recovery scenario. Vantage uses the AWS default feature for a real-time and incremental backup, by which each database instance being part of the system is automatically backed up. This allows the SRE team the restoration of the database infrastructure and customer data to a selectable point in time with a retention period of seven days. Additionally, given that the relational database service (RDS) is a regional AWS service, an additional logical backup of each database is automatically created every four hours, encrypted, and stored redundantly to mitigate any major AWS global or regional outage incident.

Whenever backups are not executed and properly stored, an incident is automatically opened and the SRE team is responsible for issue resolution following the standard incident response procedure. Additionally, the SRE team tests the recovery and restoration process at least annually.

Computer Operations - Availability

The system has been designed with redundancy, high availability, and fault tolerance as primary goals to achieve. Every service component of the system infrastructure is provisioned in multiple availability zones. In this way, impact to the Vantage service due to local outages at AWS for a specific availability zone are avoided.

Health checks are executed both at the infrastructure and software level to perform any required failover strategy whenever a specific part of the system is not working as expected.

The SRE team periodically verifies and tests that health checks have been properly set up, making sure that the related failover strategy works as expected avoiding as much as possible any kind of downtime on the system.

The SRE team provides 24x7 coverage in the case of incidents impacting the system. The monitoring tools are continuously analyzing the infrastructure and the software layers that are part of the system in real-time. If a critical problem or error is identified by these tools, an automatic incident is opened in third-party notification service (PagerDuty) and a page is automatically forwarded to the SRE team member who is on call during that specific time range.

A new incident is immediately prioritized by the SRE team and the on-call team members. The management team and internal stakeholders are updated via Slack notifications for internal purposes. For external communication to the customers a status page on the Nozomi Networks web site is updated when necessary.

When the incident has been resolved, the SRE team manages the postmortem review process, identifies, and documents the root causes of the problem. The results then shared with the development team for the purpose to identify if further follow up actions are necessary to be included in the development cycle to avoid similar problems from happening again.

Business continuity and disaster recovery plans are developed, updated, and tested annually. Additionally, backup restoration tests are also performed annually.

Change Control

Vantage uses an Infrastructure as a Code process to manage change control. Every change is written in code and follows the standard deployment procedure (commit - approve - deploy). This allows tracking of every change to the system. Manual intervention is not required except when a new environment is deployed, which happens only for new customer provisioning reasons. The creation of a new environment is documented in code.

An issue tracking system is utilized to document the change control procedures for changes in the application and implementation of new features. Development and testing are performed in an environment that is logically separated from the production environment. The authorized team reviews and approves changes prior to deployment to the production environment.

Version control software is utilized to maintain source code versions and to deploy source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes for code review purposes by the developers.

For unexpected problems or emergencies, a patch management process exists and is invoked to remediate issues immediately. The patch procedures follow the same deployment path as the code to ensure infrastructure systems are patched in accordance with vendor recommended operating system patches.

Data Communications

Network address translation (NAT) functionality is utilized to manage internal Internet Protocol (IP) addresses. Administrative access to the firewall configurations is performed in code and restricted to authorized employees. Additionally, critical data is stored in encrypted format using advanced encryption standard (AES).

Vantage is configured to utilize advanced web application protection features of the hosting provider to reduce security threats such as denial-of-service attacks.

Redundancy is built into the system infrastructure to help ensure that there is no single point of failure that includes firewalls, databases, and servers. If a primary system fails, the redundant service is configured to take its place.

Independent penetration testing is annually conducted by a reputable third-party provider to assess the security posture of the Vantage system. The approach begins with a vulnerability analysis of the target system to determine if vulnerabilities exist on the system that can be exploited via a penetration test. The test methodology includes assessment of human risks such as simulating a disgruntled or disaffected insider or an attacker that has obtained access to the system. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes application layer testing.

Vulnerability scanning is performed daily on every deploy action to identify known vulnerabilities using industry standard tools. Every finding is then tracked as an issue and processed following the standard Change Management process.

Authorized employees may access the Vantage system from the Internet. Employees are authenticated using a centralized token-based MFA system.

Boundaries of the System

The scope of this report includes Nozomi Networks' OT and IoT Security and Visibility Services System performed at the San Francisco, California and Mendrisio, Switzerland.

The scope of this report does not include the cloud hosting services provided by AWS at their multiple facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, and Confidentiality criteria were applicable to the Nozomi Networks' OT and IoT Security and Visibility Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at their multiple facilities.

Subservice Description of Services

AWS provides cloud hosting services, which include implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

Complementary Subservice Organization Controls

Nozomi Networks' services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to Nozomi Networks' services to be solely achieved by Nozomi Networks control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nozomi Networks.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	AWSCA-5.4: Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		AWSCA-5.5: Physical access points to server locations are managed by electronic access control devices.
Availability	A1.2	AWSCA-5.7: Amazon owned data centers are protected by fire detection and suppression systems.
		AWSCA-5.8: Amazon owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		AWSCA-5.9: Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon- owned data centers.
		AWSCA-5.10: Amazon owned data centers have generators to provide backup power in case of electrical failure.
		AWSCA-5.11: Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and / or customers to AWS.

Nozomi Networks management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLAs. In addition, Nozomi Networks performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Nozomi Networks' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Nozomi Networks' services to be solely achieved by Nozomi Networks' control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nozomi Networks.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls:

1. User entities are responsible for understanding and complying with their contractual obligations to Nozomi Networks.
2. User entities are responsible for notifying Nozomi Networks of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Nozomi Networks services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Nozomi Networks services.
6. User entities are responsible for providing Nozomi Networks with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Nozomi Networks of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.